North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

Marmarth dike decertified. For 50 years, a dike has protected the storied town of Marmarth, North Dakota, from flooding by the Little Missouri River. The dike remains, but it was officially decertified by federal officials in July. It will disappear from the Slope County flood map within 1 year. The Marmarth mayor said her small town has been fighting with flood officials for more than a decade over the dike's condition. Where they finally parted ways was over the gumbo clay that does not have established topsoil and vegetation. She said the U.S. Army Corps of Engineers bulldozed a bald, gumbo butte to build the levee in 1959. There have been other issues with flood officials in past years, such as fences on the dike, established trees and driving trails, but the gumbo, actually bentonite clay, was the proverbial straw. The consequence of a decertified dike is that lenders may require flood insurance for loans to build or improve property in town, which without a certified dike will be mapped as a flood plain. Source: http://www.bismarcktribune.com/news/local/article_903ac160-b545-11df-b4fb-001cc4c03286.html

Police dispose of explosive left in ND mailbox. Burleigh County authorities disposed of an explosive device that had been lit and left in a mailbox south of Bismarck, North Dakota. An official with the sheriff's office said a resident heard noises outside about 2 a.m. August 26 and later found the device, which was lit but did not detonate, in his mailbox. A Bismarck police spokesman said the department's bomb squad took an X-ray of the device then disposed of it. No one was injured in the incident. The spokesman said there are no suspects, although this is not the first explosive device reported in the area in the past few months. Authorities haven't determined whether the incidents are related. Source: http://www.grandforksherald.com/event/apArticle/id/D9HTAGJ03/

Regional

(Minnesota) **Recurring power outages are plaguing area of Coon Rapids.** Recurring power outages in the area south and west of East River Road and east of Egret Boulevard were brought to the attention of Coon Rapids, Minnesota City Council members by residents last week. The complaints were made at the Ward 3 "Summer in the City" neighborhood meeting at Al Flynn Park August 24. There was another power outage in the area served by Xcel Energy August 30. According to the city manager, following the meeting, city staff contacted the Xcel design engineer. Xcel has been aware of the recurring power outages in the area — one resident who lives on Bluebird Street said they had been taking place about every 10 days and lasting anywhere from 2 to 16 hours for the past several years — for a long time. Source: http://abcnewspapers.com/index.php?option=com_content&task=view&id=13612&Itemid=28

(Minnesota) **Dakota County sheriffs investigate copper wire thefts.** The Dakota County Sheriff's Office in Minnesota is investigating a series of copper wire thefts taken primarily from irrigation systems in southern Dakota County in the Hastings area. One additional theft involved a large amount of copper wire from a gravel pit. According to the sheriff, the thieves enter into farm fields during the

night time, stripping the copper wire that runs along the length of the irrigator which powers the wheels. This type of wire is heavy gauge and runs several hundred feet in length. Over the past several weeks, the sheriff's office has responded to five thefts with a combined loss of nearly $15,000. Typically, the copper is sold to scrap metal dealers. Additional thefts of copper have occurred in northern Goodhue County and may be related to the Dakota County thefts. The sheriff is asking residents in the rural areas of Dakota County to report any suspicious activity they see in farm fields or gravel pits. He also asks that scrap metal dealers obtain the identification of individuals attempting to sell large amounts of copper wire and to advise the sheriff's office. Source: http://www.kare11.com/news/news_article.aspx?storyid=869205

(Montana) **Safety top priority of PPL Montana after rock fall at Madison Dam.** PPL Montana is reducing water level in Ennis Lake in Ennis, Montana as the first step in a plan to assess and repair the damage caused when a large boulder, about the size of a bus, broke loose and fell onto the Madison Dam August 30. "Safety of the public and employees is the top priority as we begin the response effort," said the director of external affairs for PPL Montana. "The facility remains in a stable condition and there is no need for public action." The immediate priorities of PPL Montana are to draw down Ennis Lake to reduce pressure on the dam while experts assess the status of a large section of rock remaining on the canyon wall above the dam. PPL Montana has increased the water release rate on the lower Madison River to 3,300 cubic feet per second, which will speed the drawdown and have a limited effect on downstream recreational uses of the river. To maintain recreational uses in the upper Madison River above Ennis Lake, PPL Montana proposes no flow reductions below Hebgen Reservoir at this time. Local law enforcement officials have closed the road to the dam at Trail Creek trailhead, in effect closing the Madison River immediately downstream of the dam to recreational uses. Source: http://www.nbcmontana.com/news/24828251/detail.html

(Montana) **Davis wildfire burns 8 structures, no homes.** Officials said a 2,000-acre wildfire northwest of Helena, Montana, appears to have burned eight structures, though none were homes. A Helena National Forest agency administrator said some structures may have been piles of logs, but officials must review ownership records to be certain. An interagency team on September 1 will begin a review of the wildfire, which started as a prescribed burn that grew out of control August 26. The team will look at all factors that led up to the ignition. Fire officials said August 31 that the Davis fire is 50 percent contained. The cost of fighting the blaze is estimated to be $1.3 million. Meanwhile, the 315-acre Downing fire in the Bitterroot National Forest was 55 percent contained early August 31. Source: http://billingsgazette.com/news/state-and-regional/montana/article_cb25d9a0-b51c-11df-9a0e-001cc4c002e0.html

(Montana) **Cool temps aid Davis fire efforts.** Eight structures — none of them thought to be homes — apparently have burned in the Davis Fire near Canyon Creek, northwest of Helena, Montana. The news of the lost structures comes as the price tag of fighting the 2,015-acre wildfire has risen to $1.3 million. The change in size is due to better mapping. The Davis fire started August 25 as a prescribed burn by the Helena National Forest, but raged out of control by August 26. As of August 30, 466 people were working on the fire, which was considered 50 percent contained that evening. Source: http://helenair.com/news/local/article_2a4c70b6-b4c7-11df-9357-001cc4c03286.html

(South Dakota; Nebraska) **Fire crews contain fires in SD, western Neb.** Fire crews continue to monitor two blazes in western Nebraska and South Dakota that have scorched more than 1,200

acres. Officials with the South Dakota Wildland Fire Suppression Division said a fire southeast of Chadron, Nebraska, was contained August 28, but firefighters were still working August 29 to extinguish the blaze. Another fire west of South Dakota's Custer State Park was contained August 28 after it tore threw 65 acres. The fires were among five in the region that started August 27. A sixth was ignited the next day. Fire officials initially attributed all the fires to lightning strikes, but later said investigators determined the Nebraska fire was sparked by an all-terrain vehicle, and believed the Custer State Park fire also was human caused. Source: http://www.ksfy.com/Global/story.asp?S=13063236

National

(Texas) **Residents evacuated after big rig overturns.** A tanker truck accident had most of FM 1462 in Rosharon, Texas, closed down for hours September 2. The road was blocked off from state Highway 288 to County Road 121 for hours. People who live in the area were evacuated. The tanker truck appeared to have been pulling into a Conoco gas station when it tipped over. A second tanker has been brought in to offload the gas in the tanker. The First Baptist Church in Angleton set up a shelter for people who needed a place to go during the evacuation. Source: http://abclocal.go.com/ktrk/story?section=news/local&id=7647000

(Louisiana) **BP internal probe finds error by own engineers led to explosion, oil spill in Gulf of Mexico: report.**BP has accepted some of the blame for the deadly rig disaster in the Gulf of Mexico off the coast of Louisiana that led to the worst oil spill in United States history. An internal investigation reveals that the oil giant's own engineers misread data that contributed to the explosion aboard the Deepwater Horizon, a source familiar with BP's probe told Bloomberg News. As a result of the misinterpreted data April 20, rig workers began replacing drilling fluid in the doomed well with seawater, which was too light to prevent natural gas from leaking into the well. The report said this led to the explosion that killed 11 workers and ultimately spewed nearly 5 million barrels of oil into the Gulf of Mexico. The internal probe is one of many looking into the causes for the disaster. Other companies, including Transocean, which owned the oil rig, and Halliburton, which was working on the well prior to the blast, have also come under scrutiny. However, both companies have pointed fingers back at BP. Source: http://www.nydailynews.com/news/national/2010/08/30/2010-08-30_bp_internal_probe_finds_error_by_own_engineers_led_to_explosion_oil_spill_in_gul.html

International

Thieves steal 2 tons of explosives in Brazil. Authorities said armed men stole a truck with more than 2 tons of explosives from a chemical company in Brazil. Police said five men in two vehicles blocked the truck and held the driver hostage for several hours so they could gain time to flee. The truck's tracking system was turned off immediately after it was stolen. The army said in a statement September 2 that it will investigate whether the unnamed company had enough security measures. Police said they do not yet have enough information to link the robbery to terrorist groups or organized crime. Source: http://www.msnbc.msn.com/id/38979117/ns/world_news-americas/

Alleged ransomware gang investigated by Moscow police. Russian police are reportedly investigating a criminal gang that installed malicious "ransomware" programs on thousands of PCs and then forced victims to send SMS messages in order to unlock their PCs. The scam has been

ongoing and may have made Russian criminals millions of dollars, according to reports by Russian news agencies. Russian police seized computer equipment and detained a Russian "crime family" in connection with the crime, the ITAR-TASS News Agency reported August 31. Russian-language reports said that 10 people are expected to be charged and that tens of thousands of Russian-language victims were hit by the scam, which also affected users in Ukraine, Belarus and Moldova. The criminals reportedly used news sites to spread their malicious software, known as WinLock, which disables certain Windows components, rendering the PC unusable, and then displays pornographic images. To unlock the code, victims must send SMS messages that cost between 300 rubles (US $9.72) and 1,000 rubles. The scam is "very popular" in countries such as Russia at the moment, antivirus vendor Kaspersky Lab said in an e-mailed statement. Source: http://www.pcworld.com/businesscenter/article/204577/alleged_ransomware_gang_investigated_by_moscow_police.html

Mexico fires 3,200 federal police officers. About 3,200 Mexican federal police officers, nearly a tenth of the force, have been fired this year under new rules designed to weed out crooked cops and modernize law enforcement, officials said August 30. The housecleaning is part of the Mexican's president crackdown on drug cartels, which includes overhauling the 34,500-strong federal police force. An additional 465 federal officers have been charged with breaking the law, and 1,020 others face disciplinary action after failing screening tests, officials said. The new police standards, which took effect in May, are aimed at cleaning up Mexico's graft-plagued police force through lie detector tests, financial disclosure statements and drug testing. The government has sought to improve the caliber of federal officers by boosting wages and requiring that recruits have college degrees. The United States has backed the reform push by helping evaluate officers and supplying trainers for a state-of-the-art police academy in the city of San Luis Potosi. Source: http://www.latimes.com/news/nationworld/world/la-fg-mexico-police-fired-20100831,0,5955735.story

Hackers deface Philippine government sites. The Philippine government has asked all of its federal agencies to tighten security of their official Web sites following last week's hacking of the Philippine Information Agency (PIA) Web site, Xinhua reported. A government official said in a press statement the executive branch is adopting "best practices" to make government Web sites less vulnerable to intrusion. PIA is the official information arm of the Philippine government. The information agency Web site was down for several hours after it was hacked by a user named "7z1." The defaced Web page displayed a Chinese flag on a black background. The cyber attack was made almost a week after the Manila hostage tragedy in which eight Hong Kong tourists were killed. It is, however, unknown if the hack attack was related to the widespread public anger that followed the hostage situation. Source: http://www.thenewnewinternet.com/2010/08/30/hackers-deface-philippine-government-sites/

Cancun, Mexico, bar bombed; 8 dead. Eight people died August 31 after attackers hurled several Molotov cocktails into a Cancun, Mexico, bar, the state attorney general said. Six women and two men, all Mexican nationals and employees of the tavern, were killed in the 1:30 a.m. strike, now under investigation by judicial police, according to a release from the attorney general for the state of Quintana Roo. Eight men hurled the explosives at the bar and fled in vehicles, the release said. No shots were fired. Although the tavern is just 5 kilometers from the city's tourist stretch, it sits apart from the area frequented by tourists, and the clientele is composed of locals, it said. Four of those

slain died of burns and the others of asphyxiation, the release said. Source: http://www.cnn.com/2010/CRIME/08/31/mexico.bar.attack/index.html?hpt=T2

Finnish police arrest 30 at nuclear power plant. Finnish police arrested 30 demonstrators protesting near a nuclear power plant in Finland August 28 for refusing to follow orders, a police official said. "Police did not have an option but to detain the whole group for refusing to follow police orders," A spokesman for the Satakunta police told Agence France-Presse. "Thirty people were taken to the Rauma police station" and 10 of them were given fines, he said. The protesters started blocking roads around the Olkiluoto nuclear power plant, in southwestern Finland, early August 28. Finnish media reported that by mid-day, around 150 people were demonstrating. The confrontation with police arose when a group of protesters refused to get off the main road leading to the power plant. The protesters, some of whom came from Sweden, Germany, France, Russia and Belarus, in addition to Finland, were demanding an end to nuclear power in Finland. Source: http://www.swedishwire.com/nordic/5961-finnish-police-arrest-30-at-nuclear-power-plant

Thousands affected by flooding in southern Mexico. Authorities in Mexico's Gulf coast state of Tabasco are evacuating about 7,000 people and preparing to dig relief channels to avoid further flooding from the Grijalva River. Weeks of steady rains have caused a half-dozen rivers to overflow, partially flooding the homes or croplands of more than 60,000 people in about 200 towns. Dams in the area are near capacity. The federal government has declared a state of emergency for 12 low-laying Tabasco townships, freeing emergency funds. The state government said it would evacuate people on August 29, and authorities said relief ditches would be dug to channel water through less-populated areas to prevent flooding in the state capital, which was severely flooded in 2007. Source: http://news.yahoo.com/s/ap/20100829/ap_on_re_la_am_ca/lt_mexico_flooding

Explosion at downtown Reynosa bar. Mexican authorities are investigating an explosion at a Reynosa, Mexico, bar. The blast happened just before 1 p.m. August 28 at the La Quebradita bar near Calle Colon and Calle Juarez in the downtown area. Few details are being released. Officials were urging residents to stay away from the area. It is unknown what type of explosive device was used or if anyone was hurt. In the resort town of Acapulco, Mexico 14 bodies were discovered in different parts of the city. Mexican officials said the victims were bound, blindfolded and shot. Two bodies were found in a supermarket parking lot ,and the others were found along highways. The victims were all men ages 22 to 38 years old. Mexican officials said some of the bodies had messages left on top of them. They are suspected to have been written by drug gangs. Source: http://www.krgv.com/news/local/story/Explosion-at-Downtown-Reynosa-Bar/XLYdlWAQrEuzFgiCQ3i0nQ.cspx

Terrorism suspect employed at isotope-stocked hospital. One of several Canadian men suspected of plotting a terrorist bombing campaign worked at a hospital that houses medical isotopes that could be used in a radiological "dirty bomb," the Ottawa Citizen reported August 27. The suspect's work as an X-ray technician would not have brought him into contact with radioactive material used at the Ottawa Hospital's radiology center, hospital administrators said. The material, used in treatment of cancer and other health issues, is not kept within the part of the hospital where he worked. However, the Canadian Security Intelligence Service had officers watching the suspect at the hospital's Civic Campus, a possible sign the agency worried he might obtain sensitive material, according to the Citizen. Source: http://www.globalsecuritynewswire.org/gsn/nw_20100827_5030.php

Banking and Finance Industry

U.S. businesses could lose up to $1 billion in online banking fraud this year. Criminals who bilk businesses' online banking accounts have gotten bolder and greedier in their heists over the past year, which could ultimately result in some $1 billion in losses for U.S. companies in 2010. So said the chairman of the Anti-Phishing Working Group and CEO of IronKey: "Trend-wise, we've been looking at reports of losses since the beginning of last year at $100,000 per incident, and as we got to the latter of last year, we saw losses in the $400,000 to $500,000 range, and now we're seeing losses in the [millions range]," he said. "The majority of successful heists in cybercrime seem to be against smaller companies that tend to bank with small to midsized banks or credit unions. These banks don't have the security expertise that top banks [do] — they have the IT guy, whose also responsible for security," he said. "And many are outsourcing their banking systems to third parties, so they don't have a front-line security posture." A vice president and distinguished analyst at Gartner said $1 billion in losses from ebanking fraud for small to-midsize businesses (SMBs) is possible for this year, but that figure may be more applicable to losses over the past year and a half. It is difficult to put hard numbers on ebanking losses to SMBs and banks, she said. Source: http://www.darkreading.com/smb-security/security/attacks/showArticle.jhtml?articleID=227200174

Phishing campaign targets McDonald's fans. A widespread spam campaign that is promising cash in return for completing a McDonald's customer satisfaction survey has been uncovered. The e-mails, claiming to be sent by "McDonald's Survey Department" and with the subject line "McDonald's Customer Survey" direct recipients to the survey that poses questions on McDonald's food. Once the survey has been completed, computer users are asked to provide a raft of personal information, including their credit card number and security code, so that they can receive a $90 payment for taking the time to complete the questions. Source: http://www.net-security.org/secworld.php?id=9818

(California) **Whittier bank evacuated due to suspicious powder.** The Citibank branch at Whittwood Town Center in Whittier, California was evacuated August 31 after two employees broke out in rashes after coming in contact with a suspicious substance. The incident started at 5:15 p.m. after a person brought a bag of money into the bank at 15410 Whittier Blvd., a Los Angeles County fire captain said. Two tellers said they broke out in rashes on their forearms from a powdery substance on the money, he said. Five of the seven employees on the clock were exposed to the substance, and customers inside the bank at the time of the incident left, but were not exposed to the powder. The bank was evacuated, and at 6:46 p.m., Los Angeles County fire workers in hazardous materials suits entered the branch to test the substance. They could not determine what the substance was, according to a Los Angeles County fire inspector. Source: http://www.pasadenastarnews.com/news/ci_15956931

(Florida) **Police warn Jupiter businesses of phone scam trying to steal credit card numbers.** Police August 30 issued a warning about a scam artist who is calling Jupiter, Florida businesses pretending to be a police officer in order to extract customers' credit card information from intimidated employees. Authorities said the scammer calls up and claims he or she is either from the West Palm Beach Police Department or the FBI, then claims to need a list of the business' customers and credit card numbers as part of a fraud investigation. In at least one of the cases, the scammer has threatened to execute a search warrant on the business if the employee did not cooperate. A Jupiter police sergeant advised

business owners and employees never to give out sensitive financial information over the phone. "We don't seek out that information over the phone, even if we were conducting an investigation," he said. "If someone says they're an officer investigating something, tell them you'd be happy to cooperate but have them come in." Source: http://www.palmbeachpost.com/news/crime/police-warn-jupiter-businesses-of-phone-scam-trying-887609.html

(Illinois) **Phone scam uses credit union name as bait.** A number of Elgin, Illinois residents have reported receiving an automated phone message over the past several days, which authorities have warned is nothing more than a scam. A city spokeswoman said police received more than 30 complaints over the weekend from people reporting to have received a recorded message from someone claiming to be a representative of the Elgin-based Kane County Teachers Credit Union, 111 S. Hawthorne St. The automated message states that there is a problem with an ATM card and directs the recipient to press "1" to be connected to a security department. The KCT Credit Union vice president of marketing said the financial institution is not responsible for, or connected with, the messages being sent. She urged anyone who receives such a call never to give out any personal information, but instead contact a credit union branch directly for more information. Source: http://www.suburbanchicagonews.com/couriernews/news/2655470,3_1_EL31_04CALLS_S1-100831.article

ATM makers patch Black Hat cash-dispensing flaw. Two automated teller machine (ATM) manufacturers have shipped patches to block the cash-dispensing attack demonstrated by a researcher at the 2010 Black Hat conference. Hantle (formerly Tranax) and Triton released separate bulletins to address the issue, which lets a remote hacker overwrite the machine's internal operating system, take complete control of the ATM and send commands for it to spew cash on demand. At the Black Hat conference, the researcher demonstrated two different attacks against Windows CE-based ATMs — a physical attack using a master key purchased on the Web and a USB stick to overwrite the machine's firmware; and a remote attack that exploited a flaw in the way ATMs authenticate firmware upgrades. Source: http://www.zdnet.com/blog/security/atm-makers-patch-black-hat-cash-dispensing-flaw/7210

Chemical and Hazardous Materials Sector

(California) **Depleted uranium found at murder suspect's home.** In San Francisco, California, police are still sorting through the grisly details of a killing spree. The suspect was shot to death August 31 after a high-speed chase, and authorities found several bodies in his Vallejo home as well as chemicals, including depleted uranium. In the complicated case, it turns out a husband of one of the murder victim's was living in the murder suspect's home along with dead bodies. The husband, a chemist, is now in jail facing charges of possessing a collection of highly explosive materials authorities confiscated from the home. For the past 16 years, the husband worked as a chemical engineer at Goodrich in Fairfield, a company that makes propulsion mechanisms for all types of aircraft. Police still will not specify what chemicals were found at the chemist's home and storage unit, but the materials also included the military explosive C4, dynamite. The Bureau of Alcohol, Tobacco, Firearms and Explosives found a container labeled "depleted uranium." They are not sure what the items are until they are analyzed, said a lieutenant with the Vallejo Police Department. Source: http://abclocal.go.com/kgo/story?section=news/local/east_bay&id=7646390

U.S. NRC orders plan for reviewing safety of small modular reactors. On September 1, the Nuclear Regulatory Commission (NRC) ordered staff to complete within 6 months a plan for reviewing the safety of small modular reactors (SMRs) that will allow the agency to focus on areas of highest risk. In their order, commissioners directed staff to study "how to more fully integrate the use of risk insights into pre-application activities" in anticipation of SMR design certifications and licensing applications. With risk insights, companies and regulators can look for "areas where the largest safety risk resides" and channel resources toward areas of greatest risks, rather than imposing a blanket set of safety requirements on all designs, an NRC spokesman said. "There might be benefit in terms of streamlining or speeding up the process of considering applications," he said. SMRs are defined as reactors with capacity under 300 MW by the International Atomic Energy Agency. Reactor vendors and the U.S. Department of Energy are working on several SMR designs and the Pentagon is studying the feasibility of using SMRs to power military facilities. The NRC expects to receive the first SMR design certification application in 2012. Source: http://www.platts.com/RSSFeedDetailedNews/RSSFeed/HeadlineNews/Nuclear/6411359/

NRC considers long-term on-site storage of waste. The Nuclear Regulatory Commission (NRC) voted earlier during the month of August to explore the option of storing nuclear waste at decommissioned sites past the current 30-year standard. The NRC Chairman wrote in his vote, "The Commission has made a generic determination that, if necessary, spent fuel generated in any reactor can be stored safely and without significant environmental impacts for at least 60 years beyond the licensed life for operation." He also recommended that the staff prepare an update to the Waste Confidence Findings and Proposed Rule, "to account for storage on site storage facilities, off-site storage facilities, or both, for more than 100 years, but no longer than 300 years, from the end of licensed operations of any nuclear power plant, which may include the term of a revised or renewed license." Now that all the chairmen have voted, the Secretary of the Commission will condense the information and provide guidance for the staff, an NRC spokesman said. "It's been proven you can store this material safely on site," the spokesman said. Source: http://www.reformer.com/localnews/ci_15934549

Nation's nuclear power plants prepare for cyber attacks. The threat to digital systems at the country's nuclear power plants is considerable, but the sector is better prepared to defend against potentially devastating cyber attacks than most other utilities, according to government and industry officials and experts. Cyber attacks have been an increasing source of concern in recent years, but the threat was highlighted last month by the first discovery of malicious code, called a worm, specifically formulated to target the systems that direct the inner operations of industrial plants. To date, the malware is thought to have infected more than 15,000 computers worldwide, mostly in Iran, Indonesia and India. The issue is critically important for new nuclear power facilities that would be built in the United States and throughout the world as control rooms would employ digital systems to operate the plants. Those state-of-the-art instruments and systems make them targets for hackers. A Nuclear Regulatory Commission spokeswoman declined to say whether there have been any cyber strikes against the nation's nuclear power sector. Security events, including a computer-based attack at an energy facility, would be "sensitive information" and therefore not released to the public, she said. There have been no cyber attacks to date on U.S.nuclear facilities, according to the vice president of regulatory affairs at the Nuclear Energy Institute, a policy organization of the nuclear power and technologies industry. Source: http://www.globalsecuritynewswire.org/gsn/nw_20100827_1692.php

Commercial Facilities

(Maryland) **Discovery building hostage situation ends with suspect James J. Lee fatally shot.** A standoff at the Discovery Communications building in Silver, Spring Maryland ended September 1 when authorities shot and killed the suspect holding three hostages, bringing a dramatic close to a tense situation 4 hours after it began, according to police and law enforcement sources. All three hostages are safe and there are no reports of injuries, said the Montgomery County police chief. Sources said the suspect is a man who railed against the Discovery Channel for years. Law enforcement officials fired at 4:48 p.m. because police "believed the hostages' lives were in danger," the police chief said. Police had been negotiating with the suspect for several hours, and spoke to him minutes before firing. An explosive device the suspect had in his possession appeared to go off, the police chief said. Police were working late September 1 to clear suspicious devices in the building. The standoff began at 1 p.m. after a man walked into the large office building waving a handgun and wearing what appeared to be metallic canisters on his chest and back. The police chief said most of the 1,900 people who work in the building were safely evacuated, including all of the children at the day-care center located there. He said some employees could still be on the upper levels of the building. A different official said the suspect previously protested outside the building. In a manifesto posted on a Web site, and in newspaper ads, he excoriated the Discovery Channel and protested it because the company's programming had little to do with saving the planet. The suspect was arrested and charged with disorderly conduct after a February 2008 protest in front of the Discovery building. His probation for that arrest ended in the middle of August 2010. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and FBI officials also responded to the September 1 incident. Discovery Communications Inc. operates cable and satellite networks in 180 countries. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/09/01/AR2010090103911_pf.html

(West Virginia) **Man arrested in threat to blow up St. Albans Kroger.** A Putnam County, West Virginia, man has been arrested after threatening to blow up the Kroger in St. Albans during a failed robbery attempt. Around 4:30 p.m. August 19, a 34-year-old Scott Depot man walked up to the service desk at the Kroger on MacCorkle Avenue in St. Albans and demanded money from the clerk, according to a news release from a St. Albans Police Department official. The suspect allegedly threatened to "blow the place up," and shoot everyone in the store unless they handed over the money. The suspect did not have a weapon. He was allegedly yelling and screaming at the clerk, which drew attention from nearby shoppers at the checkout counters, according to the release. Kanawha County Metro 911 dispatcher immediately dispatched the call, highlighting the man's threat to blow up the store. St. Albans Police requested assistance from the Kanawha County Sheriff's Department bomb technicians before responding to the disturbance. Source: http://wvgazette.com/News/201008190827

(Florida) **Homes evacuated after explosives found.** About 10 homes were evacuated for a brief time August 30 after deputies discovered explosives in a duplex in Satellite Beach, Florida. At about 2 p.m., police said a 49-year-old called paramedics complaining of chest pains. As paramedics checked the house for medications, they discovered the explosives. The Brevard County bomb squad was called and removed three or four improvised explosives they found inside the home. Bomb squad officers had removed all the explosives by 10 p.m. Police said it looks like the explosives were fireworks the 49-year-old had set up for self-defense. Source:

http://www.myfoxorlando.com/dpp/news/brevard_news/083010-homes-evacuated-after-explosvies-found

(Florida) **Bomb squad removes explosive device from beach.** A portion of Phipps Ocean Park, in Palm Beach, Florida, was closed for about 2 hours August 30 until the town's bomb squad removed a 3-gallon container holding 300 meters of line and powered with solid rocket fuel that had washed ashore. The Hansson Pyrotech line-thrower was discovered by a lifeguard at about 9:20 a.m. Police and firefighters cordoned off and monitored the area until the bomb unit arrived. The device was being taken in the town's bomb trailer for disposal at the bomb range at 20 Mile Bend in Palm Beach County. Source: http://www.palmbeachdailynews.com/news/bomb-squad-removes-explosive-device-from-beach-887434.html

(Tennessee) **Authorities investigate shots fired near Islamic Center site.** Rutherford County Sheriff's deputies, the FBI, and the Bureau of Alcohol, Tobacco, Firearms and Explosives are investigating a complaint about shots being fired near the construction site of the Islamic Center of Murfreesboro, Tennessee on Veals Road off Bradyville Pike. A group of congregation members were at the site looking at the damage done to construction equipment August 28 when they heard nine shots fired from two directions. They reported hearing six shots coming from one direction, and about 3 minutes later they heard three more shots from another direction, said a congregation member and Middle Tennessee State University professor. He was not sure if the shots were being fired at the Muslim group, but in the aftermath of the weekend vandalism, he said they felt it necessary to report. Source: http://www.dnj.com/article/20100829/NEWS01/100829002/1002/Authorities+investigate+shots+fired+near+Islamic+Center+site

(Idaho) **Bomb squad detonates explosive device in N. Idaho.** Police in Coeur d'Alene, Idaho, said a bomb squad has safely detonated a briefcase containing an explosive device left several blocks from the North Idaho Fair being held at the Kootenai County Fairgrounds. Police said the briefcase was reported by a passer-by heading to the fair about 6 p.m. August 27. The briefcase had the words "Boom" and "Warning do not touch" written on it in black ink. A Spokane County, Washington, bomb squad blew up the device about 10 p.m. Police said the briefcase held some kind of explosive device, but experts may not be able to determine what kind until next week. Police said no one was injured and there was no property damage. Source: http://www.seattlepi.com/local/6420ap_id_briefcase_explosive.html

(Michigan) **Police trigger explosive device found in Emmett.** The Battle Creek Police Department Bomb Squad August 27 destroyed a small explosive device found near an Emmett Township business in Michigan. An Emmett public safety officer said the small, makeshift bomb "would have caused significant damage, but probably wasn't enough to topple a structure." The Emmett Township Department of Public Safety was called just before 6 p.m. to the Lakeside Center, a small strip mall in front of Lakeside Apartments on East Michigan Avenue, on reports of a suspicious package. Officers discovered a cylindrical object about 6 to 8 inches long in a plastic bag near the building. While fire trucks and police cars blocked off the area, the bomb squad destroyed the object with a remote-controlled device. Later investigation of the remnants revealed to police the item was a homemade bomb with a fuse. Source:

http://www.battlecreekenquirer.com/article/20100828/NEWS01/8280310/Police-trigger-explosive-device-found-in-Emmett

(Tennessee) **Fire at Tenn. mosque building site ruled arson.** Federal officials are investigating an arson-fire that started overnight August 28 at the site of a new Islamic center in a Nashville, Tennessee suburb. A special agent of the federal Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) told CBS News the fire destroyed one piece of construction equipment and damaged three others. Gas was poured over the equipment to start the fire. The ATF, FBI and Rutherford County Sheriff's Office are conducting a joint investigation into the fire. WTVF reports firefighters were alerted by a passerby who saw flames at the site. One large earth hauler was set on fire before the suspect or suspects left the scene. Digging had begun at the site, which was planned as a place of worship for the approximately 250 Muslim families in the Murfreesboro area, but no structure had been built yet. The center had operated for years out of a small business suite. Planning members said the new building, which was being constructed next to a church, would help accommodate the area's growing Muslim community. However, opponents of a new Islamic center said they believe the mosque will be more than a place of prayer; they are afraid the 15-acre site that was once farmland will be turned into a terrorist training ground for Muslim militants bent on overthrowing the U.S. government. Source: http://www.cbsnews.com/stories/2010/08/28/national/main6814690.shtml

Communications Sector

New system predicts solar storms - but ESA says satellites are safe. Researchers have developed a new method of predicting solar storms that they say could help to avoid power and communications blackouts. The next major solar storms are expected in 2012 and 2013 as part of the sun's 11-year weather cycle. A 2008 U.S. National Academy of Sciences report estimated that modern reliance on electronics and satellite communications means a major storm could cause 20 times more economic damage than Hurricane Katrina. Up to now, solar weather prediction has been carried out manually, with experts looking at 2D satellite images of the sun and assessing the likelihood of future activity. But a team from the University of Bradford's Centre for Visual Computing has now created the first online automated prediction system, using 3D images generated from the joint NASA/ESA Solar and Heliospheric Observatory satellite (SOHO). The Automated Solar Activity Prediction system (ASAP) identifies and classifies sunspots and then feeds this information through a model which can predict the likelihood of solar flares. The system is able to accurately predict a solar flare 6 hours in advance, said the team. According to the European Space Agency, there is little chance that satellites will actually be fried by solar storms. The agency is shortly to launch its first four operational Galileo satellites. Source: http://www.tgdaily.com/space-features/51348-new-system-predicts-solar-storms-but-esa-says-satellites-are-safe

(Florida) **2 charged with stealing copper wire from Collier County tower.** Information sharing between law enforcement agencies and detective work in Collier County, Florida, helped lead to the arrests of two men — including a career criminal — on multiple felony charges after deputies said the men stole copper wire from a communications tower owned by Renda Broadcasting in East Naples August 26. A 28-year-old man from Golden Gate, and a 32-year-old man from Golden Gate were each charged with burglary, grand theft $300 to $5,000 and possession of burglary tools. A search of the van turned up fresh-cut copper wire and cables, along with large bolt cutters, a pry bar and large channel lock pliers. The suspects were arrested and booked into the Collier County jail. The 32-year-

old suspect was additionally charged with two felony counts of possession of a controlled substance after deputies found a small plastic bag containing Xanax and Oxycontin pills in his possession during the traffic stop, according to arrest reports. Source: http://www.winknews.com/Local-Florida/2010-08-27/2-charged-with-stealing-copper-wire-from-Collier-County-tower#ixzz0xpEUUyh2

Critical Manufacturing

Kia recalling fire-prone cars. Hyundai-Kia Motors is recalling more than 35,000 cars with fire-prone electrical wiring systems, said the National Highway Traffic Safety Administration. The government agency said September 3 that the recall extends to some 2010-2011 Kia Soul and Kia Sorento models manufactured between Sept. 7 2009 and July 30, 2010. "When lights are illuminated under certain conditions, an electrical short may occur that can result in a fire," said the recall notice. The South Korean automaker said the faulty wiring is from the interior lighting in front and rear door trim panels, which are the plastic moldings on the inside of the car. Source: http://money.cnn.com/2010/09/03/autos/hyundai_kia_recall/index.htm?cnn=yes&hpt=T2

Ford recalling half-million minivans. Ford says it is recalling 575,000 Windstar minivans sold in the U.S. and Canada because the axles could fracture. The recall involves older models –- 1998 to 2003 –- and the carmaker said vehicles with high mileage may be especially vulnerable. In a very small number of cases, Ford said, the axles have fractured in certain locations on the right and/or left side, and affected vehicle handling. In May, a group of Ford Windstar owners filed a class action lawsuit in federal court in Pennsylvania, alleging that their vans' rear axles are rusting out, rendering the cars "unfit, unsafe, and unmerchantable." The plaintiffs said that a design defect "collects and traps water [in the axle], causing it to rust from the inside out." Specifically, the suit alleges the cylinder is hollow and unsealed, making it easy for liquid to enter, and lacks "drainage ports," meaning that the water then gets stuck inside the cylinders and has no way of getting out. The recall for the Windstar –- which is no longer in production –- applies to vehicles in 21 states, the District of Columbia, and Canada where road salt corrosion is more common. Source: http://www.consumeraffairs.com/news04/2010/08/ford_windstar.html

Defense/ Industry Base Sector

NASA tests most powerful booster rocket ever. NASA and aerospace company ATK Aerospace Systems successfully tested August 31 the most powerful solid-fuel rocket engine ever, even though its future in the space program remains in doubt. The booster, designated DM-2, was designed as the first stage of the Ares I rocket to provide the lift-off thrust for the next generation of Orion spacecraft, which NASA hoped would return astronauts to the moon by 2020. The U.S. President has said he plans to cancel the Constellation program in which the boosters would have been used, throwing the fate of the next-generation engine into question. The second test of the DM-2 was aimed at seeing if it could work at lower temperatures and verify the performance of new design materials. The solid rocket boosters are an upgrade in design over ones used to propel NASA's shuttle fleet into space, and are the largest and most powerful ever designed for flight. The second test of the DM-2, aided by more than 760 on-board measurement devices, showed the motor's performance had met all expectations. Source: http://www.space-travel.com/reports/NASA_tests_most_powerful_booster_rocket_ever_999.html

(California) **Navy's 'green' ship delayed by glitch.** The Navy's "green" ship, the San Diego, California-based Makin Island, is having mechanical trouble even before it makes its maiden deployment, though naval officials said the glitch is not related to the ship's first-of-its-kind "hybrid drive." Sailors preparing for the vessel's final check-out run in mid-August discovered that the amphibious assault ship had damage to a turning gear. The damaged part is used to prepare one of the ship's main gears by warming up the system before full operation and cooling it down after use. The repair work, being done at San Diego Naval Base, will be complete in mid-September. The glitch is pushing back the ship's final contract trials, which are designed to reveal any defects before the Navy completely accepts the ship. The final trials are usually done 6 months after the ship is received by the Navy. The Makin Island was delivered by shipbuilder Northrop Grumman in April 2009, and was commissioned in October 2009 at its home port of San Diego. Source: http://www.signonsandiego.com/news/2010/aug/30/navys-green-ship-has-glitch-not-new-technology/

Emergency Services

(California) **Investigations launched into Folsom prison riot.** Folsom State Prison in Folsom, California remains locked down and could stay that way for weeks while authorities investigate the circumstances surrounding the riot that left five inmates wounded from guards' bullets. A Folsom prison lieutenant said the situation exploded when an argument broke out between two men on the handball court in the prison's recreation yard August 27. The verbal altercation turned physical and escalated into a full-fledged melee involving more than 200 inmates. Officials called for backup from nearby California State Prison in Sacramento, to help quell the riot. When the chemical agents had little effect, guards began firing rubber bullets at the participants. When even that failed to stop the brawl, guards used conventional firearms. In all, 60 prisoners were injured. Seven inmates needed hospitalization for their wounds; five from bullet wounds and two from assault injuries. Three inmates remain hospitalized in stable condition. The fight only lasted for 6 minutes, but it took 45 staff members about half an hour to calm the crowd. The investigations into the events leaded up to the riot and the use of potentially lethal force could take weeks, and inmates could remain in lockdown until then. Source: http://cbs13.com/crime/folsom.prison.riot.2.1887468.html

(Louisiana) **Parishes make new evacuation system.** After the evacuees were out of the Monroe Civic Center in Monroe, Louisiana and all the repairs were made, local officials joined the rest of the state with lessons learned from Hurricanes Katrina and Rita. Five years later, these same local officials have partnered with other parishes to make evacuating from the south to the north as smooth as possible. They call it a point-to-point system, and the city of Monroe has already reached agreements with three parishes and devised a system that they hope will bring more structure to the evacuation process. The city of Monroe has reached cooperative endeavor agreements with Terrebonne, Lafourche, and St. John the Baptist parishes. Terrebonne Parish evacuees have been designated the Monroe Civic Center, while the Harvey H. Benoit and Emily Parker Robinson Community Centers will serve as shelter for evacuees from Lafourche Parish. Source: http://www.thenewsstar.com/article/20100830/NEWS01/8300322

(California) **California to become the first state with targeted mobile alert system.** In the next few months, California will become the nation's first state to deploy a mass mobile alerting system to alert residents and visitors in specific locations about potential emergency situations such as terrorist

attacks, wildfires, storms, child abductions, or nearby shootings. Unlike the current alerting system, which notifies individuals via cable television or calls to their landline phones, the new system can send text messages to mobile phones, and — more importantly — can target specific geographic areas, which could be as large as a city or as small as a few blocks. The system can also reach individuals who may not have landlines, may be visiting the area, or may not be in an area where they have immediate access to landlines, such as a shopping mall or sporting arena. The alerts will include vibration and an audio attention signal for wireless customers with hearing or vision disabilities. Source: http://gcn.com/articles/2010/08/26/california-mobile-alert-system.aspx

RFID no panacea for prisons. Radio Frequency Identification (RFID) systems have been frequently touted as a solution for prison systems, which can increase the efficiency of managing inmate populations, improve monitoring and control of inmates, and reduce staff time, violence, injuries and actual and attempted escapes. Despite this potential, however, there is as of yet no empirical foundation to validate claims about the technology in actual correctional environments, according to a new report. Entitled Tracking Inmates and Locating Staff with Active Radio-Frequency Identification (RFID) and prepared by the Rand Corporation and National Institute of Justice, the report documents the results of a case study of an RFID installation at the Central Detention Facility (CDF) operated by the District of Columbia Department of Corrections. "The original plan called for the design phase to last several months, with construction beginning in August 2008," the report noted. "However, for several reasons, the design phase took substantially longer than was originally anticipated, lasting until November 2008." One problem was the vendor's initial time estimate did not account for the architecture of the facility's 18 individual housing units. This failure led to inaccuracy, and the need to make modifications and test them. Also needed, the report said were "written RFID policies and operating procedures, addressing such topics as when personnel must wear an RFID unit, procedures for using RFID to control access privileges to specific areas throughout the facility, directions for inmates wearng RFID devices, and how to report problems with RFID units." Source: http://www.hstoday.us/content/view/14502/128/

Energy

Report: Nation's pipeline security uncertain. As part of DHS's mission to protect the nation's critical energy sector pipeline systems that are prime targets of terrorists such as Al Qaeda and its associated movements, the Transportation Security Administration's Pipeline Security Division (PSD) has been tasked to assess the risk and prioritize efforts to help strengthen pipeline security across the United States. But while PSA has identified the 100 most critical pipeline systems and developed pipeline risk assessment model based on threat, vulnerability and consequence, it nevertheless "could improve the model's consequence component and better prioritize its [security risk assessment] efforts," the Government Accountability Office (GAO) concluded in the report of its recent audit of PSD's pipeline infrastructure security efforts. In "Pipeline Security: TSA Has Taken Actions to Help Strengthen Security, but Could Improve Priority-Setting and Assessment Processes," GAO said that "the consequence component takes into account the economic impact of a possible pipeline attack, but not other possible impacts such as public health and safety, as called for in [DHS's] risk management guidance. PSD plans to improve its model by adding more vulnerability and consequence data, but has no time frames for doing so." GAO reviewed PSD's risk assessment process and performance measures and observed 14 PSD reviews and inspections. The government watchdog agency recommended that TSA, among other things, establish time frames for improving risk model data,

document its method for scheduling reviews, and develop a plan for transmitting recommendations to operators. Source: http://www.hstoday.us/content/view/14575/149/

Wind power is boon to Army, bane to Air Force and Navy. The military is harnessing wind to generate power at the same time that troublesome discoveries about the effects of wind turbines on radar are putting military services in conflict with clean-energy efforts. The Army's Communications-Electronics Research, Development and Engineering Center sees wind power as a key component of future portable power. CERDEC officials wrote on the "Armed With Science" blog at DODLive.mil, that as a follow-up to its Rucksack Enhanced Portable Power System effort, "CERDEC Army Power envisions the next generation of photovoltaic systems to use wind power generation as part of a hybrid system for larger-power demand applications. We call it the Reusing Existing Natural Wind and Solar System, or RENEWS." CERDEC is based at Fort Monmouth, New Jersey. Across the country, in the Mojave Desert, plans to build even more wind turbines have met with resistance from the military, who say the towers interfere with radar. "The military says that the thousands of existing turbines in the gusty Tehachapi Mountains, to the west of the R-2508 military complex in the Mojave Desert, have already limited its abilities to test airborne radar used for target detection in F/A-18s and other aircraft," the New York Times reported. Source: http://defensesystems.com/articles/2010/08/27/military-blowing-in-the-wind.aspx?admgarea=DS

(Wisconsin) **Bomb threat near power plant a bust.** Students and police gathered near the University of Wisconsin power plant at Spring and Charter Streets in Madison, August 27 to witness the detonation of a suspicious device. Madison police officers responded to a call of a suspicious package at around 5 p.m., eventually dispatching a Dane County bomb squad unit to detonate the package. Area residents were cleared to an area across the street with a clear view of the process. The bomb squad detonated the suspicious device with the assistance of a bomb-handling robot at approximately 6:45 p.m. A Madison Police Department sergeant said the device, which resembled a pipe, did not contain explosives. Police arrived at the scene after a 911 call from a Madison-area resident. She said her van was broken into the previous evening and she later discovered the suspicious pipe, which she believed could have been a homemade bomb. A University of Wisconsin Police Department (UWPD) sergeant said personnel at the scene determined the threat was contained to the block of Charter Street between Dayton and Spring streets, causing UWPD to decide against sending out a WiscAlerts message. Source: http://badgerherald.com/news/2010/08/27/bomb_threat_near_pow.php

Food and Agriculture

(California) **Shredded pork recalled in California.** Trinh Co., based in San Jose, California, is recalling approximately 2,070 pounds of cooked shredded pork skin products because they were produced without a federal inspection, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced September 1. The recall involves 8-ounce, 10-ounce and 5-pound clear plastic bags of "Trinh Co. Bi Tuoi Cooked Shredded Pork Skin, Thuong Hang Bi Tuoi V.N. Hop Ve Sinh." The recalled products were distributed to retail establishments in California. Each bag bears the establishment number "6488" inside the USDA mark of inspection. Source: http://www.foodproductdesign.com/news/2010/09/shredded-pork-recalled-in-california.aspx

(Michigan) **Antibiotic tainted beef illegally sold for human consumption.** Scenic View Dairy of Hamilton, Michigan is currently the subject of a complaint filed by the U.S. Department of Justice (DOJ) on behalf of the Food and Drug Administration (FDA) for selling beef that tested positive for illegal levels of neomycin, penicillin and sulfadimethoxine. The FDA is seeking a permanent injunction against the dairy for ignoring multiple warnings about the tainted meat. According to reports, the FDA has warned Scenic View Dairy at least eight times since 2001 about unsafe levels of antibiotics in its beef, and the USDA has sent more than 11 letters concerning the issuel. But the defendants have ignored all such warnings given between 2002 and 2010, and have continued to sell the beef. FDA regulations specify that in order to sell meat for human consumption, the animals must be off antibiotics and other drugs for a certain period of time so the substances clear from their systems. But Scenic View Dairy's three farms have allegedly been selling the meat long before the proper time. Source: http://www.naturalnews.com/029644_beef_antibiotics.html

U.S. cracks down on Chinese honey smuggling ring. The U.S. government announced criminal charges September 1 against executives from six German and Chinese companies accused of smuggling antibiotic-tainted Chinese honey in order to avoid import duties. Officials said it is the biggest food smuggling case in U.S. history and is part of a years-long crackdown on illegal imports of substandard, tainted and counterfeit products. The accused allegedly conspired to illegally import more than $40 million of Chinese-origin honey in order to avoid antidumping duties totaling nearly $80 million. The case comes after a series of scares involving Chinese products, including melamine-tainted pet food that killed scores of dogs and cats, and children's toys made with lead paint. The U.S. attorney for the Northern District of Illinois cautioned that while the honey was tainted with antibiotics that are not approved by U.S. regulators for use in honey production, there was no reason for the public to "panic." German company Alfred L. Wolff is allegedly at the heart of the conspiracy to import the mislabeled honey. It allegedly bought low-cost honey from several Chinese suppliers and then shipped it to other countries where it was filtered to "remove pollen and other trace elements that could indicate that the honey originated from China," the 44-count indictment said. Source: http://www.turkishpress.com/news.asp?id=356430

(Missouri) **68,957 pounds of cheese recalled by Mo. dairy.** More than 65,000 pounds of cheese is being recalled due to possible Listeria and Staphylococcus aureus contamination, the Food and Drug Administration (FDA) said August 30. The cheese is being recalled by Morningland Dairy of Mountain View, Missouri. Its raw milk cheese is sold in the continental U.S. in stores and by mail, as well as through crop sharing associations. The company sells its cheese in vacuum-sealed plastic packages. The FDA said the recalled codes are handwritten on the front of the package labels, ranging from A10 (representing January 1, 2010) through F250 (representing June 25, 2010). The specific brands and varieties being recalled are as follows: Morningland Dairy Raw Milk Cheese (from cow milk) Hot Pepper, garlic, Italian, and dill Colby, No salt added mild, mild, medium sharp, and sharp cheddar; and Ozark Hill Farms Raw Goat Milk Cheese, Regular, hot pepper, Italian, and garlic 'n' chive Colby, Mild, sharp, and medium sharp cheddar. Those who have bought any of these cheeses should not eat it, the FDA said, due to the possible contamination. Source: http://www.myfoxtampabay.com/dpp/consumer/68957-pounds-of-cheese-recalled-by-mo-dairy-090110

Test finds E. coli in beef faster, could better trace outbreaks. Infrared spectroscopy can detect E. coli faster than current testing methods and can cut days off investigations of outbreaks, according to a

study at Purdue University. An associate professor of food science detected E. coli in ground beef in 1 hour using Fourier transform infrared spectroscopy, much less than the 48 hours required for conventional plating technology, which requires culturing cells in a laboratory. She said spectroscopy could be done in the same laboratories, just in much less time. The spectroscopy method also differentiates between strains of E. coli 0157:H7, meaning outbreaks could be tracked more effectively and quickly. Current tests involve multiple steps and take almost 1 week to obtain results. Source: http://www.drovers.com/news_editorial.asp?pgID=675&ed_id=7790

(Iowa) **FDA reports numerous violations at egg farms.** Rodents, piles of manure, uncaged birds and flies too numerous to count were found by investigators at Iowa farms at the heart of the recall of more than half a billion eggs, the Food and Drug Administration (FDA) reported August 30. Inspection reports released by the FDA noted numerous violations at six farms operated by Wright County Egg and Quality Egg, which are owned by the same family, and three Hillandale Farms locations. The inspections — conducted in August, after new egg safety rules went into effect — were launched in response to the nationwide outbreaks of salmonella that have sickened an estimated 1,470 people, according to the FDA. Neither company fully adhered to their Salmonella enteritidis prevention plans, the inspectors said. Federal investigators found salmonella bacteria in chicken feed and in barn and walkway areas at some of the farms, officials said the week of August 23. Health officials August 30 detailed plans to launch an inspection program of these and other facilities in the coming weeks. Source: http://www.cnn.com/2010/HEALTH/08/30/eggs.salmonella/?hpt=T2

(California) **Health officials warn of tainted candy.** The California Department of Public Health warns people noto eat Cocon Grape Gummy 100 percent candy after tests found it contains high lead levels. Consumers who have the candy should throw it away. Cocon Grape Gummy 100 percent candy is manufactured by Cocon Food Industries in Malaysia, and imported and distributed by U-Can Food Trading in Los Angeles. Pregnant women aparents of children who might have eaten the candy should talk to their doctors to determine the need for medical tests. Source: http://www.pe.com/localnews/stories/PE_News_Local_D_candy28.342fa7b.html

(California; Arizona; Texas) **Frozen fruit bars recalled after typhoid outbreak.** Fruiti Pops, Inc. of Santa Fe Springs, California, has recalleits mamey (mah-MAY') frozen fruit bars because of a possible link to a rare U.S. outbreak of typhoid fever. The company said August 26 that the fruit bars were distributed in California, Arizona and Texas since May 2009. Fruiti Pops said retail stores, ice cream trucks and vending machines sold the frozen fruit bars, which have the UPC number 763734000097. The company said the frozen fruit bars were made from contaminated mamey pulp that Goya Foods, Inc. voluntarily recalled August 12after it was linked to a typhoid fever outbreak in California and Nevada. So far, no illnesses have been reported from the mamey fruit bars. Mamey or zapote, is a fruit popular in Latin America, and the Carribean. Source: http://www.google.com/hostednews/ap/article/ALeqM5jn3CmEizI31xwI8OZJiKsWBo0AD9HRFMAG2

(Louisiana; Florida) **Louisiana Gulf waters reopened for fishing.** The federal government has reopened 4,281 square miles of federal waters off the coast of western Louisiana to commercial and recreational fishing, according to the head of the National Oceanic and Atmospheric Administration (NOAA). The region being reopened represents 7.4 percent of the total area in the Gulf of Mexico that had been closed off prior to August 27. More than 48,000 square miles of federal waters roughly 20 percent of the total federal waters in the Gulf — remain closed to fishermen. At its height, the

fishing ban resulting from the April 20 BP oil rig explosistretched over 88,000 square miles, or 37 percent of federal Gulf waters. The westernLouisiana waters represent the third area in the Gulf to be reopened to fishing. A regioff the Florida peninsula was reopened July 22, and another area off the Florida panhandle was reopened August 10, according to the NOAA head. In order for an areof the Gulf to be reopened, no oil can be present or expected to be present in the forseeable future. Water samples taken from the area must pass both a sensory and chemical analysis. Source: http://www.cnn.com/2010/US/08/27/gulf.oil.disaster/

Ground beef recall affects MA BJ's wholesale Clubs. Thousands of pounds of ground beef are being recalled across the Northeast after an E. coli scare. The U.S. Department of Agriculture (USDA) said Pennsylvania-based Cargill Meat Solutions Corp is recalling 8,500 pounds of ground beef that may be contaminated. The recall is happening at BJ's Wholesale Club stores in eight states. "The ground beef that is being recalled had a use by date of July 1. If people still have the product it would likely be frozen," said a BJ's spokeswoman. "The store is going to be sending out letters to all members who purchased the item." The 42-pound cases of beef are being recalled from BJ's in Massachusetts, including Attleboro, Auburn, Leominster, Plymouth, Revere, Stoneham, Taunton, Waltham, and Weymouth. The USDA said three people have been sickened due to E. coli-related illnesses — two in Maine, and one in New York. Source: http://wbztv.com/local/ground.beef.recall.2.1885001.html

Government Sector (including Schools and Universities)

(California) **Live grenade forces evacuation of Glendale Community College campus, nearby homes.** A live Vietnam-era grenade was detonated September 2 at a Glendale Community College satellite campus in Glendale, California, according to the Los Angeles County Sheriff's Department. Investigators said the device was unearthed by construction crews at the Garfield Avenue campus. The discovery prompted the evacuation of the entire campus and several nearby residential buildings. About 450 students and about 50 instructors and other staff were evacuated from the campus. A daycare center on the campus was also evacuated and the children were sent home with their parents. John Muir Elementary School was also placed under lock down moments before the explosion. Source: http://latimesblogs.latimes.com/lanow/2010/09/grenade-glendale-los-angeles-sheriffs-department.html

(New Mexico) **Explosive device forces evacuation of nearby Los Lunas school.** Los Lunas Middle School in Albuquerque, New Mexico was evacuated September 2 as Los Lunas police investigated what they are calling an improvised explosive device. One firefighter described the device as a weird looking device containing a mysterious powder that looked like it could be potentially explosive. The device was moved by the Albuquerque Police Department bomb squad to a secure location. Source: http://www.kob.com/article/stories/S1726624.shtml?cat=504

(Virginia) **Cyber Thieves steal nearly $1,000,000 from University of Virginia college.** Cyber crooks stole nearly $1 million from a satellite campus of The University of Virginia (UVA) last week. The attackers stole the money from The University of Virginia's College at Wise, a 4-year public liberal arts college located in Wise, Virginia. According to sources familiar with the case, thieves stole the funds after compromising a computer belonging to the university's comptroller. The attackers used a computer virus to steal online banking credentials for university accounts at BB&T Bank, and initiated

a single fraudulent wire transfer in the amount of $996,000 to the Agricultural Bank of China. BB&T declined to comment for this story. Sources said the FBI is investigating and has possession of the hard drive from the controller's PC. A spokeswoman at FBI headquarters in Washington, D.C. said that as a matter of policy the FBI does not confirm or deny the existence of investigations. The attack on UVA Wise is the latest in a string of online bank heists targeting businesses, schools, towns and nonprofits. Last week, cyber thieves stole more than $600,000 from the Catholic Diocese of Des Moines, Iowa. Source: http://krebsonsecurity.com/2010/09/cyber-thieves-steal-nearly-1000000-from-university-of-virginia-college/

(Vermont) **Student threatens to blow up St. Albans school.** A Bellows Free Academy student was arrested August 27 for threatening to blow up and burn down the St. Albans, Vermont school, which was in session at the time, the St. Albans police chief said. The 16-year old boy was upset and did not have any bomb-making material, the police chief said. "These things are taken very seriously by us and the schools," he said. "I think that anytime someone makes a threat like that we have to take it seriously." Police responded to a report of an "out of control" student at the school at about 12:10 p.m. After a brief struggle, police arrested the student and cited him with false public alarm, disorderly conduct and resisting arrest. Police released him with a citation to appear in court, the police chief said. The school was not evacuated, he said. Source: http://www.burlingtonfreepress.com/article/20100831/NEWS02/100831016/Student-threatens-to-blow-up-St.-Albans-school

(California) **Bomb sqaud investigates explosives in pickup.** A bomb squad was sent to San Francisco City College in San Francisco, California August 31, because of some explosives in the back of a pickup truck. A tow truck driver was about to tow the pickup away when the owner told him there were explosives in the back. Police had the pick-up towed to the nearby city college Ocean Campus parking lot. The bomb squad roped off the area and used a robot to investigate. People with cars in the lot were told it could be a few hours before they can get them. Source: http://abclocal.go.com/kgo/story?section=news/local/san_francisco&id=7642964

(Delaware) **Delaware contractor mistakenly posts personal data of 22,000 employees.** AON Consulting, the state of Delaware's benefits consultant, mistakenly posted the Social Security numbers, gender, and birth dates of about 22,000 retired state workers on the Web 3 weeks ago, state officials and the company said August 30. According to a news report, the information was part of a request for proposal that AON had supplied to the state's procurement Web site to solicit bids from insurance companies interested in providing vision benefits to state employees and retirees. The information, which did not include the retirees' names, remained on the Web from August 16 to August 20, when the breach was discovered, the report said. A spokesman for AON said the identifying information was supposed to be "randomized" before it was forwarded to the state. "In its place should have been different identifiers, obviously nothing associated with individuals," the spokesman said, adding that the company is investigating what went wrong. The director of the Delaware Office of Management and Budget's statewide benefits office said the identifying information was not included in earlier versions of the proposal that were reviewed by her office. It only appeared in the final version, but no one spotted the change. Source: http://www.darkreading.com/database_security/security/privacy/showArticle.jhtml?articleID=227200092

(Washington) **Bomb threat forces evacuation of Grant County Courthouse Monday.** Law enforcement officers in Grant County are trying to figure out who called in a bomb threat to the courthouse in Ephrata, Washington August 30. The caller stated a person with an explosive device was going to the courthouse. About 150-people were evacuated after the call about 8:15 a.m. Sheriff's deputies, Ephrata police and Washington State Troopers secured the courthouse and conducted a room-by-room search, but nothing was found. Courthouse occupants were allowed back inside after about 1 hour. Access to the courthouse was limited for the rest of the business day to maintain security of the courthouse. Source: http://www.kndo.com/Global/story.asp?S=13070904

Air Force officials urge operational security vigilance. Fraudsters continue to hijack accounts on social networking sites and spread malicious software, FBI officials said. One technique entices users to download an application or view a video that appears to be sent from users' "friends," giving the perception of being legitimate. Once the user responds to the phishing site, downloads the application, or clicks on the video link, her computer becomes infected. With the influx of social media, Web 2.0 platforms and subsequent ease in sharing of sensitive and personally identifying information, Airmen should consider the risks and vulnerabilities in both personal and official activities, Air Force officials said. Airmen using non-classified systems must ensure they are not posting classified, restricted distribution, proprietary or For Official Use Only information on public We bsites to include Facebook, Twitter, YouTube, blog sites, etc. "We're starting to see a loss of sensitive information occurring at an alarming rate," said a spokesman from the information protection directorate. "This information not only affects the user, but can impact millions of Americans through medical, payroll and military service records." The official said release of personally identifiable information is also a concern. This includes any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history. It also includes information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, and any other personal information which can be linked or linkable to an individual. Source: http://www.afmc.af.mil/news/story.asp?id=123219924

(Tennessee) **Armed man fatally shot at Tennessee high school.** An armed man was fatally shot by deputies August 30 at a Blountville, Tennessee high school after he went inside and pointed a gun at the principal's head, a sheriff said. "There's no doubt in my mind he went there to kill someone today," the Sullivan County sheriff said at an August 30 news conference, hours after the gunfire at Sullivan Central High School. "I don't know who, and I don't know why." No students or teachers were hurt and school was dismissed at 10:30 a.m. EDT. The sheriff said the 62-year-old gunman confronted a security officer Monday morning after entering the school about 9 a.m. The gunman entered the school with a .380-caliber semiautomatic and a .25-caliber handgun in his back pocket, the sheriff said. The sheriff said that after the gunman grabbed the principal and pointed the semiautomatic at her head, a student resource officer pulled her gun on the gunman and moved the principal to safety. The suspect said the student resource officer moved the gunman down the hall and away from the cafeteria to a science pod. When Sullivan County deputies arrived, they ordered the gunman to drop his weapon, and he allegedly pointed it in their direction. He then pointed it back toward the school resource officer, prompting deputies to fire, the sheriff said. Source: http://www.google.com/hostednews/ap/article/ALeqM5hXDrr4xADS5PSc21wuDgH1LK2XswD9HU25J01

Ex-Army analyst from OK. arrested at Minn. airport. A former U.S. Army analyst from Oklahoma was arrested in Minneapolis, Minnesota while trying to board a one-way flight to China with electronic files containing a restricted Army field manual, authorities said August 27. Federal prosecutors said the 26-year-old suspect allegedly was carrying multiple data storage devices when he was arrested August 26 at the Minneapolis-St. Paul International Airport. The suspect was charged August 26 in Oklahoma City with one count of theft of government property, which carries a maximum sentence of 1 year in prison. The defense attorney said the charge is a misdemeanor. The suspect made his initial appearance in U.S. District Court in St. Paul, Minnesota, August 27. A detention hearing was scheduled for August 30 to determine when the suspect will be returned to Oklahoma, said a spokesman for the U.S. Attorney's Office in Oklahoma City. The suspect worked as an analyst at Oklahoma's Fort Sill until August 16, when his clearance was revoked due to security violations, according to an FBI affidavit in the case. The affidavit did not disclose the nature of the violations. Source: http://www.google.com/hostednews/ap/article/ALeqM5gtoVQcxQo_WywP0PHdUxmKDtqDDwD9HS3LO00

(Pennsylvania) **Man charged with threatening to shoot Congresswoman's staff.** A Philadelphia man is in federal custody after allegedly threatening to shoot members of a Pennsylvania Congresswoman's staff, according to reports August 28. The FBI said the 44-year-old suspect called the Congresswoman's office August 25 regarding his lost dentures and complained the Congresswoman has never done anything for him despite always getting his vote. When he did not get the response he wanted, the suspect told the staff member on the phone that he was a former Marine with access to a rifle. He then threatened to get on a bus, stand on the roof across the street, and shoot staff members in the Congresswoman's Philadelphia office. The suspect later called back and spoke with a second staff member and told them he was a patient at Aria Hospital in Philadelphia. When an FBI agent went to interview the suspect at the hospital, he had already been discharged. Hospital officials had expressed concern about his mental state but were unable to commit him for a psychiatric evaluation without his consent. Later that night FBI agents visited the suspect's apartment accompanied by his girlfriend and arrested him. The U.S. Attorney's office said the suspect will be detained pending a psychiatric evaluation and a hearing to see if he is competent to stand trial. Source: http://thehill.com/blogs/blog-briefing-room/news/116225-man-charged-with-threatening-to-shoot-congresswomans-staff

U.S. analyst is indicted in leak case. A federal grand jury in Washington D.C. has indicted a State Department analyst suspected of disclosing top-secret information about North Korea to Fox News, the third time the Obama administration has filed criminal charges accusing people of leaks to the news media. The indictment, dated August 19 and unsealed August 27, named a specialist in nuclear proliferation who worked as a contractor for the State Department. The suspect, who has worked as a high-level foreign affairs analyst for a decade for various federal agencies, is accused of disclosing the information in June 2009 and of lying to the FBI in September 2009. The analyst pleaded not guilty August 27 in federal district court, and was released on $100,000 bond. A person familiar with the investigation said it involved a Fox News report on North Korea's likely reaction to a United Nations Security Council resolution, which was then pending, that condemned its nuclear and ballistic missile tests. Fox News said at the time that it was "withholding some details about the sources and methods by which American intelligence agencies learned of the North's plans." Source:

http://www.nytimes.com/2010/08/28/world/americas/28leak.html?src=un&feedurl=http://json8.nytimes.com/pages/world/americas/index.jsonp

Crime or espionage? Zeus is a well known crimeware tool kit that is readily available online. Typically, Zeus has been associated with banking fraud. Recently, there have been a series of attacks using the Zeus malware that appear to be less motivated by bank fraud and more focused on acquiring data from compromised computers. The themes in the e-mails — often sent out to .mil and .gov e-mail addresses — focus on intelligence and government issues. After the user receives such an e-mail, and downloads the file referenced in the e-mail, his or her computer will likely (due to the low AV coverage) become compromised by the ZeuS malware used by the attackers and will begin communicating with a command and control server. It will then download an additional piece of malware, an "infostealer," which will begin uploading documents from the compromised computer to a drop zone under the control of the attackers. What appears to be a one-off attack using Zeus, the author believes, is actually another round of a series of Zeus attacks. These attacks appear to be aimed at those interested in intelligence issues and those in the government and military, although the targeting appears to be general rather than targeted. Details of such an attack were recently posted on contagiodump.blogspot.com. The e-mail used in the attack appeared to be from "ifc@ifc.nato.int" with the subject "Intelligence Fusion Centre" and contained links to a report EuropeanUnion_MilitaryOperations_EN.pdf that exploits CVE-2010-1240 in order to drop a Zeus binary. Source: http://www.infowar-monitor.net/2010/08/crime-or-espionage/

Information Technology and Telecommunications

IPv6 transition poses new security threats. The countdown to the saturation of the IPv4 address supply is now down to a matter of months: and along with the vast address space of the next-generation IPv6 architecture comes more built-in network security as well as some new potential security threats. IPv6 has been in the works for over a decade now, but with the exhaustion of the IPv4 address space expected anywhere from spring to June of 2011, the long transition to the new IP may finally be on the radar screen for some organizations. Unlike its predecessor, the "new" protocol was built with security in mind: it comes with IPSec encryption, for instance, and its massive address space could help prevent worms from propagating, security experts said. But its adoption also poses new security issues, everything from distributed denial-of-service (DDoS) attacks to new vulnerabilities in IPv6 to misconfigurations that expose security holes. Some experts expect implementing DNSSEC in an IPv6 network to be simpler than in existing IPv4 networks. "It eases the transition to DNSSEC. IPv6 lets you migrate to DNSSEC much more easily than trying to do so on an old IPv4 stack. The concern with DNSSEC has been you've got a lot of legacy IPv4 equipment out there, and some of it is non-standard, which is very difficult" to integrate with DNSSEC, said the COO of Lumeta. Source:
http://www.darkreading.com/vulnerability_management/security/perimeter/showArticle.jhtml?articleID=227300083&subSection=Perimeter+Security

SQL injections dominated malware in 2010, as Gumblar botnet named as 'the most significant malware development in years'. The number of IPS SQL injections increased substantially in the second quarter of 2010 following a downturn. Cisco's global threat report for the second quarter revealed IPS SQL injection signature firings increased substantially in the period to coincide with outbreaks of SQL injection-compromised Web sites. It also claimed Asprox SQL injection attacks made

a reappearance in June of 2010, after nearly 6 months of inactivity. A senior security researcher at Cisco said: "SQL reappears in this period, but we can predict with some certainty where the next wave of SQL injections are coming from using our statistics." The report also found that 7.4 percent of all Web-based malware encounters in the first quarter of 2010 resulted from search engine queries, while nearly 90 percent of all Asprox encounters in June of 2010 were the results of links in search engine results pages. The researcher noted the data was collected from actual user clicks, and not overall detections. "This is based on actual users who encountered malware and on actual events ... we are reporting on actual events and I see that as a high figure and the only one that tops it is Gumblar." The Gumblar "botnet" of compromised Web sites was first detected by ScanSafe as a collection of Web sites being used to distribute Web-based malware. Asked if it was still active, the Cisco researcher called it "the most significant malware development in years." She said: "We took notice of trusted Web sites and the themes on the Web site, and Gumblar took it to a new level with botnets of compromised Web sites." Source: http://www.scmagazineuk.com/sql-injections-dominated-malware-in-2010-as-gumblar-botnet-named-as-the-most-significant-malware-development-in-years/article/178186/

Google releases Chrome 6 with 14 security updates. Google has released a new version of its Chrome browser and has included more than a dozen security fixes in the update. The new version, 6.0.472.53, was released 2 years to the day after the company pushed out the first version of Chrome. Google Chrome 6 includes patches 14 total security vulnerabilities, including six high-priority flaws, and the company paid out a total of $4,337 in bug bounties to researchers who reported the vulnerabilities. A number of the flaws that didn't qualify for bug bounties were discovered by members of Google's internal security team. The new release of Chrome also fixes an older bug, a Windows kernel flaw, that Google had thought it fixed in a previous version. The highest bug bounty, $1,337, was paid for the user who discovered an integer error in WebSockets. A second high-priority flaw, a sandbox parameter deserialization error, was discovered by two members of Adobe's Reader Sandbox Team. This is the first major release of Chrome since Google increased the rewards it pays to researchers who identify bugs in the browser. None of the bugs fixed in Chrome 6 qualified for the maximum reward of $3,133.7, which Google said it will pay out for bugs deemed to be SecSeverity Critical. Source: http://threatpost.com/en_us/blogs/google-releases-chrome-6-14-security-updates-090210

New Zeus campaign uses FedEx notice scam. Security firm McAfee has alerted the online community to a new Zeus botnet attack using bogus FedEx notification e-mails. McAfee malware research scientist made note of the new Zeus push August 31 in a McAfee Labs blog posting. The scientist said the new spam campaign is linked to the Asprox botnet, which is spreading e-mails that use FedEx branding. The research scientist said these fake FedEx e-mails contain attachments that are really executables, with file names starting in FedExDoc or FedExInvoice. "Those attachments are recognized as the Bredolab Trojan," wrote one Malware research scientist, "which will download the Zeus component." Zeus is the notorious Trojan delivered via e-mail files with .exe attachments, and is designed to make off with personal and banking information. Malware research scientist also added that several large U.S. banks are among targets of the fake FedEx e-mails –- including Citibank, Comerica, USBank and Wells Fargo –- in addition to several other banks in Europe, the Middle East, Asia, and South America. Source: http://www.infosecurity-us.com/view/12149/new-zeus-campaign-uses-fedex-notice-scam/

Fake antivirus software using ransom threats. Fake antivirus programs appear to be adopting some of the money-raising tactics of more threatening ransom malware, security company Fortinet's latest threat report has found. The most prevalent malware variant during August was TotalSecurity W32/FakeAlert.LU!tr, a malicious program that masquerades as antivirus software in order to sell worthless licenses for non-existent malware. On its own, it accounted for 37.3 percent of all malware threats detected by the company during the month. Unlike standard fake antivirus programs, however, the new version of TotalSecurity takes the ruse a stage further by preventing any applications other than a Web browser to run, claiming they are "infected." The user is invited to have the infection cleaned by buying the bogus TotalSecurity product. "This is another example of how relying purely on antivirus is not a silver-bullet approach to protecting systems from infection," said Fortinet's threat research head. Source: http://www.networkworld.com/news/2010/090210-fake-antivirus-software-using-ransom.html?hpg1=bn

Apple patches 13 iTunes security holes. Apple has shipped a new version of its iTunes media player to fix 13 security flaws that cold be exploited to launch attacks against Windows machines. The patches in the new iTunes 10 covers vulnerabilities in WebKit, the open-source Web browser engine. The WebKit vulnerabilities, already patched in Safari, expose Windows users to remote code execution attacks via maliciously crafted Web sites. The iTunes 10 update is available for Windows 7, Windows Vista and Windows XP SP2 or later. Source: http://www.zdnet.com/blog/security/apple-patches-13-itunes-security-holes/7252

Botnet takedown may yield valuable data. Researchers are hoping to get a better insight on botnets after taking down part of Pushdo. An assistant professor of computer science at Ruhr-University in Bochum, Germany said his group is working on an academic paper focused on methods to figure out what type of malicious spamming software is on a computer that sent a particular spam e-mail. He said they found that Pushdo had a special characteristic in that more than half of its command-and-control servers were concentrated within one hosting company. About 15 of Pushdo's 30 servers were with that one hosting provider, which has now taken those servers offline and shared the data contained within them with the researcher and his team. Their analysis is still ongoing, but they uncovered some 78 GB of plain text e-mail addresses, and found that up to 40 percent of the infected computers were in India. Of the eight hosting providers that had Pushdo's command-and-control servers, six took action to shut Pushdo down. But two hosting providers based in China did not respond to e-mail requests to turn off Pushdo or even acknowledged that they had received a complaint, the researcher said. Source: http://www.computerworld.com/s/article/9183299/Botnet_takedown_may_yield_valuable_data

New zero-day vulnerabilities imminent. An independent group of security researchers has announced that they will be releasing zero-day vulnerabilities, Web application vulnerabilities, and proof-of-concept (POC) exploits for patched vulnerabilities throughout September. Many high-profile vendors such as Adobe, Apple, Microsoft, and Mozilla are among those whose products will apparently have vulnerabilities revealed during the month. According to a Trend Micro researcher, the vulnerabilities to be announced refer to a collection of old and new ones primarily targeting Microsoft. The new vulnerabilities can be considered zero-day flaws and will leave users vulnerable until a vendor patch is offered and applied. However, the process may take some time. Until then, users should use any suggested workarounds. It is also believed that detailed information for recently released advisories will be published. It is possible the data released includes POC code, making

exploits more likely. Exploit packs on malicious and compromised Web sites will probably include these new exploits as well. Any new information released during this period will likely be quickly exploited, putting more users at risk. High-profile applications like Internet Explorer (one of the programs that the researchers have indicated they will release a vulnerability for) can have exploit code released within hours of the POC code's announcement. Portions of the many exploits already in the wild can be reused in any new exploit attack, further hastening the process. Source: http://blog.trendmicro.com/new-zero-day-vulnerabilities-imminent/

Corporate espionage for dummies: HP scanners. Web servers have become commonplace on just about every hardware device from printers to switches. Despite typically being completely insecure, such Web servers on printers/scanners are generally of little interest from a security perspective, even though they may be accessible over the Web, due to network misconfigurations. A researcher was recently looking at a newer model of an HP printer/scanner combo and something caught his eye. HP has for some time, embedded remote scanning capabilities into network aware scanners, a functionality referred to as Webscan. Webscan allows one to not only remotely trigger the scanning functionality, but also retrieve the scanned image, all via Web browser. The feature is generally turned on by default with absolutely no security whatsoever. With over $1B in printer sales in Q3 2010 alone, and with many of the devices being all-in-one printers, running across an HP scanner in the enterprise is certainly very common. What many businesses do not realize, is that their scanners may by default allow anyone on the LAN to remotely connect to the scanner and if a document was left behind, scan and retrieve it using nothing more than a browser. As everything is Web based, an enterprising but disgruntled employee could simply write a script to regularly run the scanner in the hopes of capturing an abandoned document. Source: http://www.net-security.org/article.php?id=1484

Apple QuickTime backdoor creates code-execution peril. A security researcher has unearthed a "bizarre" flaw in Apple's QuickTime Player that can be exploited to remotely execute malicious code on Windows-based PCs, even those running the most recent versions of operating system. Technically, the inclusion of an unused parameter known as "_Marshaled_pUnk" is a backdoor because it is the work of an Apple developer who added it to to the QuickTime code base and then, most likely, forgot to remove it when it was no longer needed. It sat largely undetected for at least 9 years until a researcher of Spain-based security firm Wintercore discovered it and realized it could be exploited to take full control of machines running Windows 7, Microsoft's most secure operating system to date. "The bug is pretty bizarre," the CSO of Rapid7 and chief architect of the Metasploit project told The Register August 30. "It's not a standard vulnerability in the sense that a feature was implemented poorly. It was more kind of a leftover development piece that was left in production. It's probably an oversight." The presence of _Marshaled_pUnk creates the equivalent of an object pointer that an attacker can use to funnel malicious code into computer memory. Source: http://www.theregister.co.uk/2010/08/30/apple_quicktime_critical_vuln/

Google disputes bug patching report. Google August 30 said that a recent report claiming it failed to patch a third of the serious bugs in its software had the facts wrong. IBM's X-Force security company, which released the report last week, acknowledged the error and issued a revised chart that shows Google patched all the vulnerabilities rated "critical" or "high" in its online services. "We questioned a number of surprising findings concerning Google's vulnerability rate and response record, and after discussions with IBM, we discovered a number of errors that had important implications for the

report's conclusions," said a security program manager at Google in an entry on a company blog. Recently, X-Force's report claimed that 9 percent of all Google bugs disclosed in the first half of 2010 were unpatched, and 33 percent of the vulnerabilities ranked as critical or high had not been fixed. According to IBM's revised tabulations, Google patched every vulnerability revealed in the first 6 months of this year.
Source:http://www.computerworld.com/s/article/9182818/Google_disputes_bug_patching_report

Badly configured networks believed to be the main cause of network breaches. Misconfigured networks account for more than three quarters of breaches. A survey found that a badly configured network is the main cause of network breaches because IT professionals "don't know what to look for." The survey, conducted by Tufin, also revealed that 18 percent of security experts believe misconfigured networks are the result of insufficient time or money for audits, while 14 percent felt that compliance audits that do not always capture security best practices are a factor. The CTO and co-founder of Tufin said: "The really big question coming out of the survey is how to manage the risk that organizations run dealing with the complexity that is part and parcel of any medium-to-large sized company's security operations. Almost half of the respondents (43 percent) also claimed that planting a rogue member of staff inside a company was one of the most successful hacking methodologies. However, 58 percent of attendees said they did not believe outsourcing security to a third party increased the chances of getting hacked, and almost half the sample believe it would not increase the chances of any sort of security or compliance issue. Source:
http://www.scmagazineuk.com/badly-configured-networks-believed-to-be-the-main-cause-of-network-breaches/article/177911/

Too many disclose sensitive information on social networks. Social networking users should be careful when accepting friend requests, and must be conscious of the data they share. According to a new study by BitDefender, social network users do not appear to be preoccupied with the real identity of the people they meet online or about the details they disclose while chatting with total strangers. The study revealed that 94 percent of those asked to "friend" the test profile, an unknown, attractive young woman, accepted the request without knowing who the requester really was. The study sample group included 2,000 users from all over the world registered on one of the most popular social networks. These users were randomly chosen in order to cover different aspects: sex (1,000 females, 1,000 males), age (the sample ranged from 17 to 65 years with a mean age of 27.3 years), professional affiliation, interests etc. In the first step, the users were only requested to add the unknown test profile as their friend, while in the second step, several conversations with randomly selected users aimed to determine what kind of details they would disclose. The study showed that more than 86 percent of the users who accepted the test-profile's friend request work in the IT industry, of which 31 percent work in IT Security. It also found the most frequent reason for accepting the test profile's friend request was her "lovely face" (53 percent.) After a half an hour conversation, 10 percent disclosed personal sensitive information, such as: address, phone number, mother's and father's name, etc –- information usually requested as answers to password recovery questions. Two hours later, 73 percent siphoned what appears to be confidential information from their workplace, such as future strategies, plans, as well as unreleased technologies/software. Source:
http://www.net-security.org/secworld.php?id=9793

National Monuments and Icons

(Massachusetts) **Campers evacuate as Cape prepares for Earl.** Residents in Cape Cod, Massachusetts took final preparations September 2 for the impending arrival of Hurricane Earl. Even after the sun went down the work continued as people pulled their boats from the water before the hurricane arrived. At Ryders Cove in Chatham, more than 150 boats were pulled from the water September 2. Campers were forced to leave Nickerson State Park in Brewster by 5 p.m. September 2 as Earl approaches. The American Red Cross is prepared in case they need to put up some shelters along Cape Cod, and if necessary, they could house up to 10,000 people a night. Source: http://www1.whdh.com/news/articles/local/12002115827857/campers-evacuate-as-cape-prepares-for-earl/

(Colorado) **Marijuana field discovered in Boulder Co.** Boulder County Sheriff's deputies in Colorado uncovered a marijuana grow operation on U.S. Forest Service land west of Lyons August 30, and authorities were looking for two suspects they described as "heavily armed." Deputies were acting on a tip when they found the field, comprised of roughly 3,000 marijuana plants, near Raymond and Riverside. A spokesperson said a suspect, described only as a Hispanic male, fled from the scene when officers arrived, disappearing into the Roosevelt National Forest. Agents were searching the area for the suspect and additional marijuana fields. Source: http://www.kwgn.com/news/kdvr-pot-field-boulder-txt,0,7639165.story

Postal and Shipping

(Florida) **Suspicious package closes park.** Edgewater, Florida city workers found a box containing bottles and aerosol cans at Menard May Park September 2 and called police. An officer with military experience in Iraq indicated the package was suspicious. "The fuse coming out of it was a hint," one officer said. Six hours later, police rendered the device safe with a small, controlled blast. No one was hurt. Investigators have "indicators that it was" a bomb but were conducting lab tests on debris. The Bureau of Alcohol, Tobacco, Firearms and Explosives and local police were working together to identify "who built the device and what it was intended to do." Source: http://www.news-journalonline.com/news/local/southeast-volusia/2010/09/03/suspicious-package-closes-park.htm

(Oklahoma) **Suspicious device found in Ardmore church.** On September 2, the bomb squad was called in Ardmore, Oklahoma, after authorities say an improvised explosive device was left in the parking lot of Northwest Baptist Church. The bomb squad destroyed the device. No one was hurt, and there were no evacuations. So far, no suspects have been arrested. The Ardmore Police and the Oklahoma Highway Patrol Bomb Squad are still investigating. Source: http://www.kten.com/Global/story.asp?S=13093544

(Indiana) **FedEx truck explodes.** A FedEx truck exploded, caught fire, and tumbled down a hill, all in a matter of minutes. Around 1:30 p.m. September 1, the driver of the truck was traveling on North Red Bank in Evansville, Indiana when he noticed smoke coming from the back of the truck. He got out and attempted to use an extinguisher, but the fire was already fully engulfed. Firefighters said aluminum from the truck melted to the road and some power lines were damaged. A FedEx representative tells

FOX 7 there were only a handful of packages still on board and the driver was not injured. The cause of the fire is under investigation. Source: http://tristatehomepage.com/fulltext?nxd_id=193305

(South Carolina) **Post office to remain closed until testing complete.** Postal officials said that a Greenwood, South Carolina post office closed because of a strange smell August 30 will remain closed until tests are complete. A spokesman for the United State Postal Service said that on August 27, workers at the North Creek Boulevard office began complaining of irritation to their eyes, skin and throat. He said several workers left early to seek medical attention. The spokesman said that air-quality tests were performed over the weekend, but they did not reveal any cause of the smell. He said a National Guard team was called in to conduct further tests and that team completed their assessment August 30. Crews found insecticide in some carpet at the office. The spokesman said that after completing their tests, crews felt safe enough to be inside the building without protective equipment. He said test results from a state lab and an independent air quality company will be completed before the building is reopened. He added that the building would undergo a minimum 24-hour cleanup before it is reopened. During the downtime, the spokesman said that customers can pick up their mail or buy postal products at the Magnolia Avenue post office. Source: http://www.foxcarolina.com/news/24829889/detail.html

(Nevada) **Lyon County Courthouse evacuated because of suspicious envelope.** The Lyon County Courthouse in Yerington, Nevada was evacuated for nearly 4 hours August 26, and the bomb squad from the Fallon Naval Air Station was called to investigate after a suspicious envelope was delivered to the district attorney's office. The Lyon County emergency management director, who is serving as the interim county manager, said he ordered the evacuation of the courthouse, the courthouse annex and the administrative complex on the advice of the U.S. Bureau of Alcohol, Tobacco and Firearms after the package was received at about 11:45 a.m. Lyon County's deputy emergency management coordinator said the envelope was delivered to the district attorney's office, and drew suspicion because of its appearance. The emergency management director said the envelope turned out to contain some sort of a hate letter. Source: http://www.rgj.com/article/20100901/FERNLEY01/9010333/1306/FERNLEY

(Texas) **Feds arrest Texan in powder-filled letters hoax.** Federal agents have arrested a Dallas man for allegedly mailing white powder-filled envelopes to Internal Revenue Service and social security offices in Texas and Maryland. The 51-year-old suspect, who was taken into custody August 26, appeared before a federal magistrate August 27, the U.S. Attorney for the Northern District of Texas said in a statement. It was not immediately known whether the suspect had an attorney. Investigators said they do not believe the suspect is responsible for sending threatening letters containing suspicious white powder to several U.S. embassies and governors' offices 3 years ago. They said they also doubt he recently sent 30 more such letters to churches, mosques and aeronautical and technical businesses in Texas, Illinois and Massachusetts. Source: http://www.dallasnews.com/sharedcontent/APStories/stories/D9HS53702.html

PUBLIC HEALTH

(Indiana) **Human West Nile cases confirmed in Indiana.** The Indiana State Department of Health said September 3 that the first two confirmed cases of West Nile virus of the season were confirmed this week. One of the cases is in Marion County, and the other is in Allen County. The public relations

coordinator of the Marion County Health Department (MCHD), said the department has been performing tests on mosquitoes in the county for 6 months. Central Indiana usually records human cases from late August through the end of the mosquito season, which generally happens at the first hard frost. "While not surprising, these human cases serve to remind all of us that mosquitoes with the West Nile virus are active and we must remain vigilant in protecting ourselves," said MCHD's director. Five people have died from West Nile virus in Marion County since 2002, with 52 human cases recorded. Source: http://www.theindychannel.com/health/24869530/detail.html

SmartMetric's biometric card to provide personal medical records. SmartMetric said that its fingerprint activated Biometric Data Card can be now used to provide the highest level of both security and portability for a person's medical history and full medical records. The SmartMetric Data Card can store Gigabytes of medical information including full EKGs, complete CT and MRI digital images, and similar data making up an individual person's complete medical records. Storage of digital images, in particular, requires significant digital storage capacities. Unlike other systems that are severely limited in the amount of digital data that can be held in a portable solution, The SmartMetric solution provides security for the patients information in that it can only be accessed after the patient touches the surface sensor on the Health Card triggering the Card to scan the persons fingerprint and matching it with their fingerprint pre-stored inside the card. Only after a finger print verification internally in the card is the data able to be accessed or viewed by a doctor, hospital or EMT's computer. Source: http://www.tmcnet.com/usubmit/2010/09/02/4987396.htm

(Indiana) **St. Vincent ER evacuated due to suspicious car.** The morning of August 31, the emergency room at St. Vincent Hospital in Indianapolis, Indiana, on West 86th Street was evacuated due to a report of an unknown vehicle in the parking lot. The car was unoccupied and parked at the front entrance to the emergency room (ER). Metro police, along with the fire department and bomb squad, were called in as a precaution. After careful examination of the car, officials said they found nothing suspicious. During the search, some people were moved out of the ER area and into other areas of the hospital. An "all clear" was issued, and the situation is back to normal according to a source within the hospital. Source: http://www.fox59.com/news/wxin-st-vincent-er-evacuated-083110,0,7166511.story

Pentagon Pulls $1B from WMD-Defense Efforts to Fund Vaccine Initiative. The U.S. Defense Department has shifted more than $1 billion out of its nuclear, biological, and chemical defense programs to underwrite a new White House priority on vaccine development and production to combat disease pandemics, according to government and industry officials. The planned funding reduction "terminates essential CBRN [chemical, biological, radiological and nuclear] defense programs ... required to meet high priority service needs, prevent casualties and protect against CBRN incidents," according to a Pentagon budget document drafted in early August. Internal deliberations over the budget have been ongoing for months as the government prepares to submit its fiscal 2012 spending request to Congress next February. Source: http://www.globalsecuritynewswire.org/gsn/nw_20100827_5297.php

(New York) **Hunt for suspect who planted suspicious black bag at Westchester Medical Center.** Detectives are hunting for the person who left a black bag of medical waste with a threatening message for police at the Westchester Medical Center campus in Valhalla, New York August 29. The bag was spotted outside the Behavioral Health Center, and drew police, firefighters and hazardous

materials experts, including the Westchester County bomb squad. Police would not say what message was written on the black bag, except that it was a threat to police. Inside the bag was medical waste. It was not immediately clear where it came from, police said. It was the second suspicious package to draw a large emergency response in three days. On August 27, a silver package left on train tracks in Irvington was blown up by police using a water cannon without determining exactly what it was, although officials said it was not an explosive. Source: http://www.lohud.com/article/20100830/NEWS02/8300346/-1/newsfront/Hunt-for-suspect-who-planted-suspicious-black-bag-at-Westchester-Medical-Center

TRANSPORTATION

(California) **4 arrested in train trespassing sweep.** Four people were arrested September 2 on suspicion of trespassing on Union Pacific railroad property in southern California as local authorities looked for trespassers on private railroad property. The operation, which stretched from Camarillo to Montalvo, involved the Oxnard Police Department, the Ventura County Sheriff's Department, the Los Angles County Sheriff's Department, DHS, and agents from the Union Pacific Police Department. Agents and police also were looking for pedestrians, motorists and bicyclists who failed to yield the right of way or obey train crossing signs and warnings at train track crossings. Officers said they witnessed 60 different violations. California ranked second in the nation in 2009 for collisions at train track crossings, with 121 accidents. Of these, 91 resulted in death. Moreover, 61 of these collisions were fatal trespasses and 42 were trespasses with injuries. Source: http://www.vcstar.com/news/2010/sep/02/4-arrested-in-train-trespassing-sweep/

(New York) **LIRR to suspend service on two branches as Hurricane Earl nears.** With Hurricane Earl expected to bring tropical-storm conditions to the New York metropolitan area, the Long Island Rail Road moved to suspend service on its two East End branches starting September 3. The service suspension means that thousands of New Yorkers who ride the Montauk and Ronkonkoma Branch trains to the Hamptons and the North Fork had to find other ways to the beach for Labor Day weekend. Service was suspended east of Speonk on the Montauk Branch and east of Ronkonkoma on the Ronkonkoma Branch. LIRR officials were worried that high winds from Hurricane Earl would snap crossing gates, down trees and knock out power lines. "We don't want a train with a thousand people on it that can't proceed because of a broken gate or a broken wire or down trees," said an LIRR spokesman. Source: http://blogs.wsj.com/metropolis/2010/09/02/lirr-to-suspend-service-on-two-branches-as-hurricane-earl-nears/

(New York) **2 charged with lying in probe of N.Y. Amtrak attack.** Federal prosecutors have charged two people with lying during an investigation of an attempt to sabotage an Amtrak line on Indian territory in Irving, New York. The FBI has been probing a July 5 incident in which an Amtrak train carrying 354 passengers hit a barricade of railroad ties on the Seneca Nation's Cattaraugus Territory south of Buffalo. The train was moving at 70 mph, but damage wasn't severe and no one was hurt. Federal prosecutors said their probe has focused on four men who walked along the tracks after leaving a party. Source: http://www.wcax.com/Global/story.asp?S=13060709

(Georgia) **Woman shot at Delta facility in Atlanta.** A woman carrying a gun and apparently looking for a Delta Air Lines employee was shot and killed outside the airline's maintenance facility August 31. An autopsy will be conducted today to determine if she fatally shot herself or if a Clayton County

police officer killed her, a spokesman said. The woman was shot in a sedan inside a secure, employee parking lot at Delta's technical operations center at Hartsfield-Jackson International Airport. It's unclear if she had a security badge or forced her way into the facility. "[She] was looking for a Delta employee who was not at work," said a police officer, who said the shooting was related to a domestic situation. Source: http://www.securityinfowatch.com/Executives/1317397

(Colorado) **Copper thief leaves I-25 motorists in the dark.** Thanks to a copper thief, Colorado motorists on Interstate 25 will remain "in the dark" when it comes to travel time between Castle Rock and Colorado Springs. The thief stole copper wiring out of a conduit at a Colorado Department of Transportation (CDOT) facility near Larkspur. That conduit was part of a network of five "smart signs" which tell motorists the travel time to the next city. "Those signs were supposed to be activated by Labor Day weekend," said a CDOT spokesman. "That date has been pushed back about 2 weeks." The smart signs cost taxpayers $630,000. CDOT is spending an additional $40,000 to replace the wiring and to repair the damage. Source: http://www.thedenverchannel.com/news/24828025/detail.html

(Florida) **Palm Beach airport cleared after bomb threat.** A concourse at Palm Beach International Airport was evacuated for about 1 hour August 30 as officials investigated a bomb threat. The Transportation Security Administration said the threat targeted a flight to New York's LaGuardia Airport. Passengers disembarked as authorities inspected the plane and luggage. Flights were allowed to resume and passengers returned to the concourse after officials determined the threat wasn't credible. Source: http://www.miamiherald.com/2010/08/31/1800233/palm-beach-airport-cleared-after.html

(California) **Lasers force 2 Coast Guard helicopters to land at LAX.** Two Coast Guard helicopters were forced to land at Los Angeles International Airport (LAX) in the last week after being flashed with laser beams, the latest of 63 such incidents reported near the airport so far this year, and part of a growing problem nationwide. Someone flashed a laser at a Coast Guard helicopter flying over San Pedro's Cabrillo Beach about 9 p.m. August 26, forcing the crew to make a precautionary landing at LAX, said a Coast Guard petty officer. Another Coast Guard helicopter was flashed with a laser August 24 while flying over Torrance. It also had to land. In both incidents, crew members were grounded until a doctor cleared them to fly again. Aiming laser beams in pilots' eyes is illegal and can cause temporary blindness. Federal Aviation Administration officials said the aiming of high-powered beams at aircraft is a growing problem. They said the number of such cases has risen dramatically nationwide since the early 2000s. The agency has logged 1,525 laser incidents this year, a big jump from the 283 reported in 2005. Source: http://www.latimes.com/news/local/la-me-faa-laser-20100829,0,15935.story

(Pennsylvania) **Lasers pointed at two STAT MedEvac helicopters.** The Federal Aviation Administration was notified after lasers were pointed at two STAT MedEvac that were flying north of Pittsburgh, Pennsylvania, a STAT MedEvac official told a Pittsburgh-area television station. A manager for STAT MedEvac said in an e-mail to the news station that the lasers were green in color. No one was injured and there was no damage. Source: http://www.post-gazette.com/pg/10241/1083560-100.stm

Water and Dams

(Nebraska) **Landowner fined for improper dam.** The Environmental Protection Agency (EPA) has fined a northeast Nebraska landowner and an excavation company $30,000 for building a dam without proper authorization. EPA said the owner of Norfolk, Nebraska, hired Custom Excavation of Madison, Nebraska to build an earthen dam. The U.S. Corps of Engineers discovered the dam last fall on a tributary of Spring Branch Creek. The EPA said the dam affected more than 1 mile of the creek and more than 1 acre of nearby wetland. Landowners are required to consult with the Corps of Engineers and obtain permits before building dams. The EPA said the landowner is working with officials to develop a restoration plan for the area. Source: http://www.omaha.com/article/20100831/NEWS01/708319891

(Michigan) **EPA to focus on source of PCB spill.** Environmental Protection Agency (EPA) officials said August 26 they plan to shift focus from cleaning up PCB toxins in sewer drains and some canals off Jefferson Avenue in St. Clair Shores, Michigan, to finding the source of the decade-long contamination. "Finding the source is our primary focus before we look at a remedy," the remedial project manager for the EPA said during a public meeting. Federal, state and local officials have spent more than $10 million to purge the compound from the canals and groundwater. Now, the EPA could place the 10 Drain site on the federal Superfund list next month, which would make it eligible for millions in funding. The project manager said they plan underground field sampling, including in areas around the drain. That work would take place early in 2011. Many of the close to 100 residents told the EPA they were tired of waiting for answers. Polychlorinated biphenyls (PCB) were found in the 10 Mile Drain area in 2001 when the county collected sediment samples for a proposed dredging project. Toxins have been concentrated in canals behind Lange and Revere streets. The chemicals were banned in the 1970s. Source: http://www.detnews.com/article/20100827/METRO03/8270367/1412/METRO03/EPA-to-focus-on-source-of-PCB-spill

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**


NDDES
Homeland Security
State Radio
NORTH DAKOTA
STATE PATROL
NORTH DAKOTA
STRENGTH FROM THE SOIL
NATIONAL GUARD